UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/689,596	10/22/2003	Donald Yang	BHT-3212-46	6109

7590 03/20/2007

TROXELL LAW OFFICE PLLC
SUITE 1404
5205 LEESBURG PIKE
FALLS CHURCH, VA 22041

EXAMINER	
ABYANEH, ALI S	
ART UNIT	**PAPER NUMBER**
2137	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/20/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/689,596	YANG ET AL.	
	Examiner	Art Unit	
	Ali S. Abyaneh	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 December 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-40* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-40* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *22 October 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-25 are presented for examination.

Objections

2. Claims 13-21 objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. For example claim 14 depends on claim 15, claim 15 depends on claim 14 and claim 21 depends on itself.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless -
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1,4,5,11,12, 16,22,31-33 and 36-40 are rejected under 35 U.S.C. 102(e) as being anticipated by Kessler et al. (US Patent NO. 7,170,999).

Regarding claim 1, 12 and 31

Kessler teaches a digital information protecting method for encrypting a piece of digital information from an author computer (column 2, lines 27-28) with assistances from a server (column 2, lines 31-31), and then transmitting an encrypted digital information to a client computer via a computer network for the client computer to decrypt the encrypted digital information to be used (column 2, lines (column 2, lines 35-40), both the author computer and the client computer comprising a predetermined information processing software to process the piece of digital information, the method comprising: in the author computer: receiving a content key from a server and encrypting the piece of digital information by the content key (column 2, lines 27-33); encrypting the content key by a predetermined key encrypting process; and transmitting the encrypted digital information and the encrypted content key to the client computer (column2, lines 37-40); and in the client computer: decrypting the encrypted content key by a corresponding predetermined key decrypting process; and decrypting the encrypted digital information by the content key to make the piece of digital information can be used by the client computer (column 6, lines 47-65).

Regarding claim 4, 5, 16

Kessler further discloses a method, wherein the information processing software of the author computer comprises a plurality of

universal keys with encoded serial number; and wherein the key encrypting process is executed the following steps by the information processing software of the author computer: choosing one of the plurality of universal keys, and encrypting the content key by the chosen universal key, and storing the encrypted content key and the serial number of the universal key to a header, and adding the header in front of the encrypted digital information (column 9, line 54-column 10, line 49).

Regarding claim 11, 22, 39 and 40

Kessler further discloses a method, wherein the information processing software encrypts and decrypts the piece of digital information by Advanced Encryption Standard; (AES) method; wherein the content key is encrypted and decrypted by Advanced Encryption Standard (AES) method; and wherein the public key and the private key are encrypted and decrypted by Rivest Shamir Adleman (RSA) method (column 6, lines 57-65).

Regarding claim 32

Kessler further discloses wherein the content encrypting module and the key encrypting module are set in an author computer, and the content decrypting module is set in a client computer (column 2, lines 22-42).

Regarding claim 33

Kessler further discloses, wherein the key decrypting module is set in a server (column 2, lines 34-35).

Regarding claim 36 and 37

Kessler further discloses, server transmits the public key to the author computer; and wherein the public key transmitted from the server is acquired from an issue device (column 2, lines 34-35).

Regarding claim 38

Kessler further discloses a claim, wherein the encrypted content key are stored in a header, and added the header in front of the encrypted digital information (column 9, line 54-column 10, line 49).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) patent may not be obtained though the invention is not identically disclose or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 2, 3, 6-10, 13-15, 17-21, 34 and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kessler et al. (US Patent NO. 7,170,999), in view of Pensake et al. (US Pub NO. 2001/0052074).

Regarding claim 2, 13, 34

Kessler teaches all limitation of the claim as applied to claim 1 above. Kessler does not explicitly teach, wherein the author computer draws up a policy relating to the piece of digital information, and transmits the policy to the server. However, in an analogous art, Pensak teaches, wherein the author computer draws up a policy relating to the piece of digital information, and transmits the policy to the server (paragraph [0040]). Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Kessler to include the author computer draws up a policy relating to the piece of digital information, and transmits the policy to the server. This would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to do so in order to provide access to encrypted information by authorized user and furthermore to provide a method and system for encrypting electronic information so that access to the information can be controlled by the author or other controlling party (paragraph [0005]).

Regarding claim 3, 14, 35

Pensake further discloses a method, wherein the policy comprises the range, time, and using times of the piece of digital information being authorized (paragraph [0040]).

Regarding claim 6, 17

Kessler teaches all limitation of the claim as applied to claim 1 and 16 above. Kessler does not explicitly teach, wherein before the information processing software of the author computer executes the key encrypting process, the software asks the author of the author computer to authorize an Off-line Access Permission. However, in an analogous art, Pensak teaches wherein before the information processing software of the author computer executes the key encrypting process, the software asks the author of the author computer to authorize an Off-line Access Permission (paragraph [0040]). Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Kessler to include, before the information processing software of the author computer executes the key encrypting process, the software asks the author of the author computer to authorize an Off-line Access Permission. This would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to do so in order to provide access to encrypted information by authorized user and furthermore to provide a method and system for encrypting electronic information so that access to the information can be controlled by the author or other controlling party (paragraph [0005]).

Regarding claim 7, 18

Pensake further discloses, wherein the Off-line Access Permission determines whether the client computer is permitted to process and use the received piece of digital information in the off-line situation (paragraph [0040]).

Regarding claim 8-10, 15 and 19-21

Kessler further discloses, wherein the key decrypting process is executed the following steps by the information processing software of the client computer: getting a corresponding universal key according to serial number stored in the header; and decrypting the content key by the universal key; and wherein the information processing software of the client computer downloads the universal key from the server according to the serial number; and wherein the information processing software of the client computer comprises a plurality of universal keys, the information processing software of the client computer chooses corresponding universal key according to the serial number (column 9, line 54-column 10, line 49).

7. Claim 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kessler et al. (US Patent NO. 7,170,999), in view of Andivahiset al. (US Patent NO. 7,146009).

Regarding claim 23

Kessler teaches A digital information protecting method for encrypting a piece of digital information from an author computer with assistances from a server, and then transmitting an encrypted digital information to a client computer via a computer network for decrypting the encrypted digital information to be used, the method comprising: in the author computer, encrypting the piece of digital information by a content key (column 2, lines 27-33); in the author computer, encrypting the content key by a public key; in the author computer, transmitting the piece of encrypted digital information and the encrypted content key to the client computer (column2, lines 37-40); in the client computer, receiving the piece of encrypted digital information and the encrypted content key; and in the client computer, decrypting the piece of encrypted digital information by the decrypted content key (column 6, lines 47-65). Kessler does not explicitly teach transmitting the encrypted content key to the server; in the server, decrypting the encrypted content key by a private key corresponding to the public key; in the server, transmitting the decrypted content key to the client computer. However in an analogous art Andivahiset teaches transmitting the encrypted content key to the server; in the server, decrypting the encrypted content key by a private key corresponding to the public key; in the server, transmitting the decrypted content key to the client computer (column 2, lines 30-45). Therefore it would have been obvious to one having ordinary skill in the art at the time

the invention was made to modify Kessler to include transmitting the encrypted content key to the server; in the server, decrypting the encrypted content key by a private key corresponding to the public key; in the server, transmitting the decrypted content key to the client computer. This would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to do so in order to provide a secure communication of electronic messages and electronic data stream amongst a community of user (column 1, lines 48-51).

8. Claims 24-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kessler et al. (US Patent NO. 7,170,999), in view of Andivahiset al. (US Patent NO. 7,146009), further in view of Pensake et al. (US Pub NO. 2001/0052074).

Regarding claim 24

Kessler and Andivahiset teach all limitation of claims as applied to claim 23 above. Kessler and Andivahiset do not explicitly teach, wherein the author computer draws up a policy relating to the piece of digital information, and transmits the policy to the server. However, in an analogous art, Pensak teaches, wherein the author computer draws up a policy relating to the piece of digital information, and transmits the policy to the server (paragraph [0040]). Therefore it would have been obvious to

one having ordinary skill in the art at the time the invention was made to modify Kessler and Andivahiset to include the author computer draws up a policy relating to the piece of digital information, and transmits the policy to the server. This would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to do so in order to provide access to encrypted information by authorized user and furthermore to provide a method and system for encrypting electronic information so that access to the information can be controlled by the author or other controlling party (paragraph [0005]).

Regarding claim 25

Pensake further discloses a method, wherein the policy comprises the range, time, and using times of the piece of digital information being authorized (paragraph [0040]).

Regarding claim 26 and 27

Kessler further teaches, server transmits the public key to the author computer; and wherein the public key transmitted from the server is acquired from an issue device (column 2, lines 34-35).

Regarding claim 28

Kessler further teaches, where in encrypted content key are stored in a header, and added the header in front of the encrypted digital information (column 9, line 54-column 10, line 49).

Regarding claim 29 and 30

Kessler further teaches a method, wherein the content key is encrypted and decrypted by Advanced Encryption Standard (AES) method; and wherein the public key and the private key are encrypted and decrypted by Rivest Shamir Adleman (RSA) method (column 6, lines 57-65).

References Cited, Not Used

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

1. U.S. Publication No. 2002/0021804

This reference relates to a method for data encryption, secure transmission and decryption.

Conclusion

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ali Abyaneh whose telephone number is (571) 272-7961. The examiner can normally be reached on Monday-Friday from (8:00-5:00). If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone numbers for the organization where this application or proceeding is assigned as (571) 273-8300 Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR)

system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ali Abyaneh AA
Patent Examiner
Art Unit 2137
03/15/07

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER